

Presentation of Specification to TSG

Presentation to: TSG SA Meeting #20

Document for presentation: TS 23.240, Version 2.0.0

Presented for: Approval

Abstract of document:

The 3GPP Generic User Profile (GUP) is the collection of user related data which affects the way in which an individual user experiences services and which may be accessed in a standardised manner.

3GPP TS 23.240 defines the stage 2 architecture description to the GUP, which includes the elements necessary to realise the stage 1 requirements in 3GPP TS 22.240. 3GPP TS 23.240 includes the GUP reference architecture with descriptions of functional entities, and their interfaces and procedures, as well as the high-level information model for the GUP data.

Changes since last presentation to TSG-SA:

Both the proxy and redirect modes of operation of the GUP Server have been selected. The Rg reference point procedures have been added. GUP information model and Rp reference point procedure descriptions have been enhanced. Descriptions of authentication, authorisation, privacy control, synchronisation and location of profile components have been made more detailed.

Outstanding Issues:

Inclusion of the existing profile components in the Generic User Profile. Effect of the authorisation and privacy related enhancements on the GUP information model.

Contentious Issues:

None

3GPP TS 23.240 V2.0.0 (2003-05)

Technical Specification

**3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
3GPP Generic User Profile - Architecture;
Stage 2
(Release 6)**



The present document has been developed within the 3rd Generation Partnership Project (3GPP™) and may be further elaborated for the purposes of 3GPP.

The present document has not been subject to any approval process by the 3GPP Organizational Partners and shall not be implemented. This Specification is provided for future development work within 3GPP only. The Organizational Partners accept no liability for any use of this Specification. Specifications and reports for implementation of the 3GPP™ system should be obtained via the 3GPP Organizational Partners' Publications Offices.

Keywords

<User, Profile, Architecture>

3GPP

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

<http://www.3gpp.org>

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© 2003, 3GPP Organizational Partners (ARIB, CWTS, ETSI, T1, TTA, TTC).
All rights reserved.

Contents

Foreword.....	5
Introduction.....	5
1 Scope	6
2 References	6
3 Definitions, symbols and abbreviations.....	6
3.1 Definitions.....	6
3.2 Symbols.....	6
3.3 Abbreviations.....	6
4 Reference Architecture.....	7
4.1 GUP Functionalities	7
4.1.1 Harmonised access interface	7
4.1.2 Single Point of Access.....	7
4.1.3 Authentication of profile access	7
4.1.4 Authorisation of profile access	7
4.1.5 Privacy Control.....	7
4.1.6 Synchronisation of data storage.....	7
4.1.7 Access of profile from visited network	8
4.1.8 Location of Profile Components.....	8
4.1.9 Charging for Profile Access	8
4.2 GUP Functional Entities.....	8
4.2.1 GUP Server.....	9
4.2.1.1 Single Point of Access.....	11
4.2.1.2 Location of Profile Components.....	11
4.2.1.3 Authentication of Profile Request	11
4.2.1.4 Authorisation of Profile Request	11
4.2.1.5 Synchronisation of Profile Components.....	12
4.2.1.6 Additional Functionality.....	12
4.2.2 Repository Access Function (RAF).....	12
4.2.3 GUP Data Repository.....	12
4.2.4 Reference Points	12
4.2.5 Applications.....	12
4.2.6 Message Flow of using GUP	13
4.3 Rg reference point procedures.....	15
4.3.1 Create procedure.....	16
4.3.2 Delete procedure.....	16
4.3.3 Modify procedure	17
4.3.4 Query procedure	18
4.3.5 Subscribe procedure	18
4.3.6 Unsubscribe procedure	19
4.3.7 Notify procedure.....	19
4.3.8 Common information definitions	20
4.3.8.1 Requestor data	20
4.3.9 Error handling and common error types	20
4.4 Rp reference point procedures.....	21
4.4.1 Create Component procedure	21
4.4.2 Delete Component procedure	22
4.4.3 Modify Data procedure.....	22
4.4.4 Read Data procedure	23
4.4.5 Subscribe To Data procedure	23
4.4.6 Unsubscribe To Data procedure	24
4.4.7 Notify Data procedure	24
4.4.8 Define Data procedure.....	25
4.4.9 Common information definitions	25
4.4.9.1 Requestor data	25

4.4.10 Error handling and common error types25

5 GUP Information Model..... 26

Annex A (informative): Examples of 3GPP Generic User Profile Usage 29

Annex B (informative): 3GPP Generic User Profile candidates 30

Annex C (informative): Change history 33

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
 - 1 presented to TSG for information;
 - 2 presented to TSG for approval;
 - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

The fact of having several domains within the 3GPP mobile system (e.g. Circuit-Switched, Packet-Switched, IP Multimedia Subsystem) and access technologies (e.g. GERAN, UTRAN and WLAN) introduces a wide distribution of data associated with the user. Further, the new functions both in terminals and networks mean that the data related to users, services and user equipment will be increased greatly. This causes difficulties for users, subscribers, network operators and value added service providers to create, access and manage the user-related data located in different entities.

The objective of specifying the 3GPP Generic User Profile is to provide a conceptual description to enable harmonised usage of the user-related information located in different entities. Technically the 3GPP Generic User Profile provides an architecture, data description and interface with mechanisms to handle the data.

1 Scope

The present document defines the stage 2 architecture description to the 3GPP Generic User Profile (GUP), which includes the elements necessary to realise the stage 1 requirements in 3GPP TS 22.240 [1].

The present document includes the GUP reference architecture with descriptions of functional entities, and their interfaces and procedures, as well as the high-level information model for the GUP data.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TS 22.240: "Stage 1 Service Requirement for the 3GPP Generic User Profile (GUP)".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document the following definitions apply:

3GPP Generic User Profile (GUP): The 3GPP Generic User Profile is the collection of user related data which affects the way in which an individual user experiences services and which may be accessed in a standardised manner as described in this specification.

GUP Component: A GUP component is logically an individual part of the Generic User Profile.

Data Element: the indivisible unit of Generic User Profile information.

Data Element Group: A pre-defined set of Data Elements and/or other Data Element Groups closely related to each other. One or more Data Element Groups can constitute the GUP Component.

Data Description Method: A method describing how to define the data contained in the Generic User Profile.

3.2 Symbols

For the purposes of the present document the following symbols apply:

Rg	Reference Point between Applications and the GUP Server.
Rp	Reference Point between the GUP Server and GUP Data Repositories, and between Applications and GUP Data Repositories.

3.3 Abbreviations

For the purposes of the present document the following abbreviations apply:

GUP	3GPP Generic User Profile
RAF	Repository Access Function

4 Reference Architecture

4.1 GUP Functionalities

4.1.1 Harmonised access interface

The GUP harmonized access interface is the interface which can be used by the GUP suppliers and GUP consumers to access, manage and transfer the profile data. This application layer interface is independent of the profile structure.

4.1.2 Single Point of Access

There exists for each Profile a single point of access, which knows the location of the various components of the Profile.

4.1.3 Authentication of profile access

A GUP functionality exists that is responsible to authenticate applications. Authentication is a vital function to be passed before any kind of access to GUP data is granted. GUP shall adopt generic mechanisms such as used for the OSA framework approach.

4.1.4 Authorisation of profile access

A GUP functionality exists that is responsible to authorise applications to access GUP data based on User specific privacy rules. All attempts to access the GUP data are to be authorised according to the defined policies which shall include the requestor's identity.

The GUP data structures need to satisfy the requirement to provide the authorisation information on the different levels: profile, component or data element. In addition to the generic authorisation data, additional service specific data may be defined (e.g. for LCS). The same applies for the authorisation decision logic. How the generic decision logic is defined and provided is FFS.

Both HPLMN based applications and non-HPLMN based applications are expected to send requests to the GUP Server. The GUP server shall have functionality to apply different authorisation criteria, policy control and load control to HPLMN and non-HPLMN applications. Policy control and load control are out of the scope of the present document.

4.1.5 Privacy Control

The tight connection of Authentication, Authorisation and subscriber specific privacy requirements results in Privacy control. Privacy control implies a centralized management for access rights including the subscriber's privacy requirements.

4.1.6 Synchronisation of data storage

The GUP data repository holds the master copy of the GUP component data. Applications or GUP server may copy (i.e. read) the component data or request synchronisation. The present document defines how the data is requested and sent. What is thereafter done with the data by the application or GUP server is beyond the scope of the present document.

Synchronisation means that the changes to the master copy of the data are propagated to the entities that request synchronisation. The synchronisation request specifies which data are monitored for changes. It is also possible to request that all changes are reported.

Synchronisation may cause heavy processing load to the involved entities, thus some policies are required in the implementations but those are not specified for the time being. However the GUP interfaces should carry sufficient data for enabling the load control mechanisms to work.

The entity under a heavy processing load has the responsibility to handle the error cases and conditions and to reach the synchronisation as fast as possible. All the unresolved errors or load balancing actions that affect synchronisation shall be reported.

4.1.7 Access of profile from visited network

Access to GUP from a visited network shall follow the single point of access principle.

4.1.8 Location of Profile Components

A GUP functionality exists that keeps information where GUP data are located.

4.1.9 Charging for Profile Access

The GUP Server shall be capable of providing charging information, e.g. to enable transaction/event based charging.

Some GUP Data Repositories may provide charging information, while other GUP Data Repositories do not provide charging information.

Mechanisms are needed to permit the GUP Server to know which GUP Data Repositories are (and are not) producing their own charging information. When the GUP Data Repository is capable of producing charging information, mechanisms are needed for the correlation of the charging information produced by GUP Server and GUP Data Repository.

NOTE: GUP Data Repositories within a UE are not expected to produce charging information.

The charging information may also be used for other event logging, customer care, privacy auditing, etc. functions.

4.2 GUP Functional Entities

The GUP reference architecture as shown in Figure 4.1 consists of:

- GUP Server;
- Repository Access Function (RAF);
- GUP Data Repositories;
- Rg and Rp reference points;
- Applications.

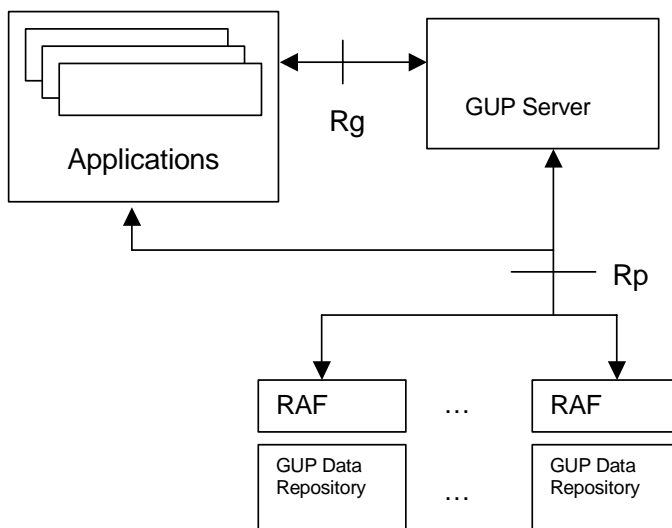


Figure 4.1: GUP Reference architecture

An example of mapping the GUP reference architecture to current infrastructure environment is shown in Figure 4.2.

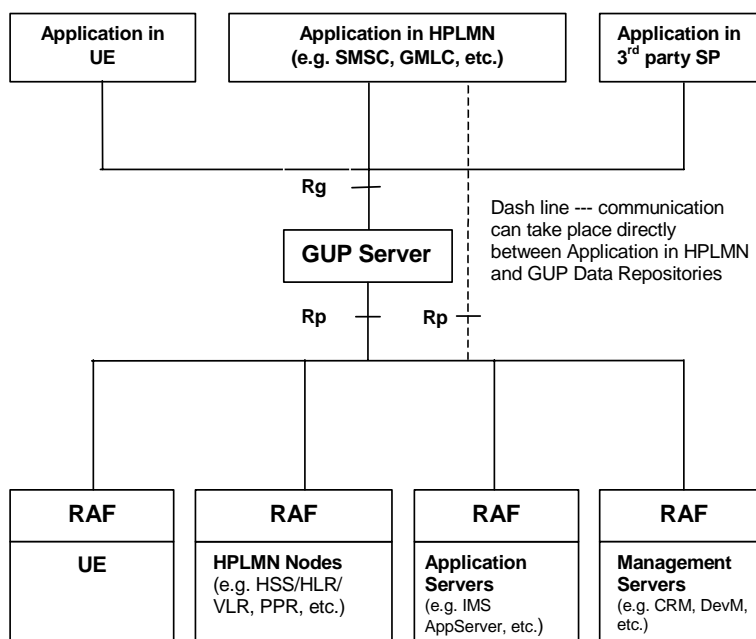


Figure 4.2: An example of mapping the GUP reference architecture to Current Infrastructure Environment

4.2.1 GUP Server

The GUP Server is a functional entity providing a single point of access to the Generic User Profile data of a particular subscriber. The Reference Architecture does not specify or limit the physical location of the GUP Server enabling flexibility in the implementations.

The GUP Server includes the following main functionalities:

- Single point of access for reading and managing generic user profile data of a particular subscriber.

- Location of Profile Components.
- Authentication of profile requests.
- Authorisation of profile requests.
- Synchronisation of Profile Components.

The GUP Server shall support two modes of operation:

- **Proxy mode** (see figure 4.3). The Application requests user related data located in the GUP Data Repositories from the GUP Server. After taking care of needed actions specified for the GUP Server (and depending on the type of the request) the GUP Server makes requests to the corresponding GUP Data Repositories and receives responses from them. Finally the Application gets a response to the original request from the GUP Server. Depending on the type of the request also possible subsequent responses are delivered through the GUP Server.
- **Redirect mode** (see figure 4.4). The Application requests user related data located in the GUP Data Repositories from the GUP Server. After taking care of needed actions specified for the GUP Server (and depending on the type of the request) the GUP Server returns to the Application the information (e.g. address of GUP Data Repository(s)) to allow the Application to request the information from the GUP Data Repositories. The Application then directly requests the information from the GUP Data Repositories.

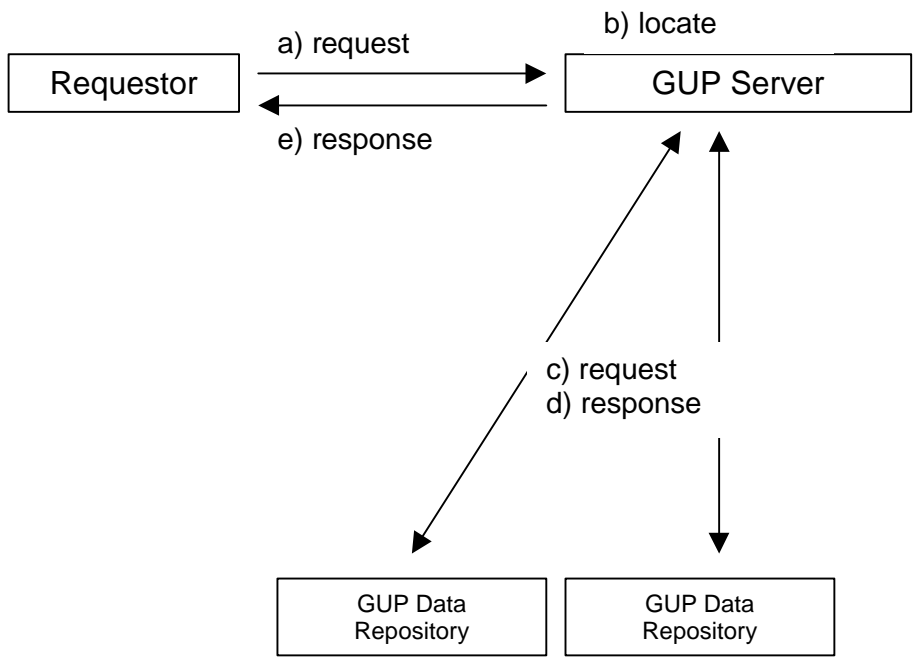


Figure 4.3: GUP Server acting as a Proxy Server.

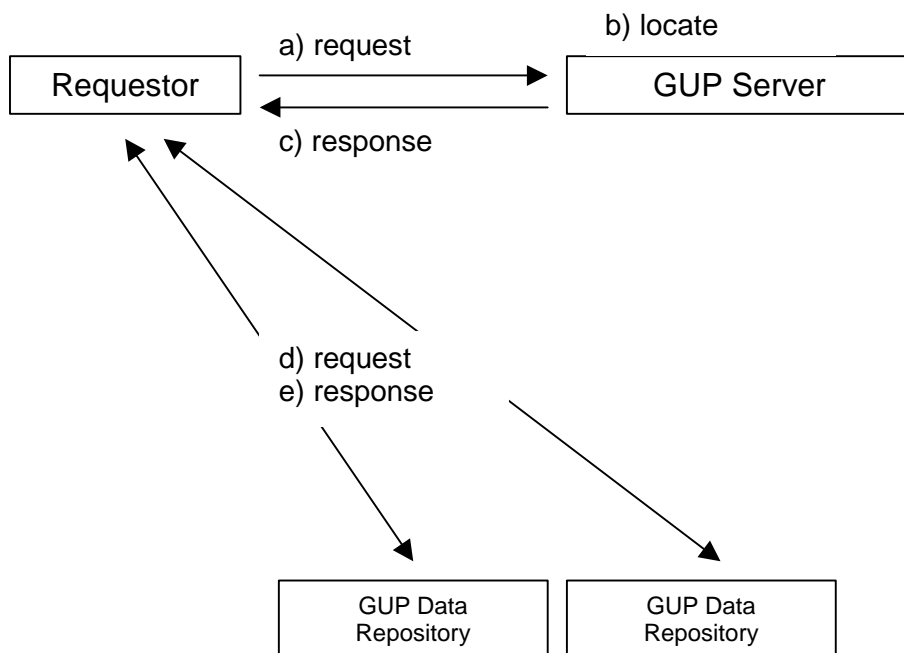


Figure 4.4: GUP Server acting as a Redirect Server.

4.2.1.1 Single Point of Access

The GUP Server shall accept data management related requests from the applications via the Rg reference point, and either convey the corresponding GUP Component specific requests to GUP Data Repositories via Rp reference point or redirect the Application to convey the requests to the GUP Data Repositories. Note that one data request from an application to the GUP Server can cause sending of several GUP Data Repository requests by the GUP Server or Application. Also mapping to proprietary interfaces instead of Rp is possible in implementations.

In Proxy mode the GUP Server shall receive the results of the requests from GUP Data Repositories and deliver the results back to the requestor (application). In case of responses from several GUP Data Repositories the GUP Server shall combine separate XML documents received from the repositories and deliver the composed information to the requestor. In redirect mode the Application will receive the results of the requests from the GUP Data Repositories.

4.2.1.2 Location of Profile Components

The GUP Server stores information about the GUP Components and the locations of data repositories of GUP Components related to each subscriber. Thus e.g. the separate GUP Components composing the whole User Profile of a certain subscriber can be located and identified. It is beyond this specification how the GUP server gets the component locations in the cases when it is not involved in the creation of those components.

4.2.1.3 Authentication of Profile Request

The GUP Server shall make sure that the application requesting user profile data is properly authenticated. The authentication is based on the identification of the requesting application and/or the identification of the possible subscriber requesting the user profile data. The GUP Server may rely on the authentication made by other trusted entities.

4.2.1.4 Authorisation of Profile Request

The GUP Server shall take care of the authorisation of the access to the user profile data. The authorisation itself may be handled by a separate entity in the network, or alternatively by the RAF or GUP Data Repository. The authorisation shall be based on the requestor information, the requested data, the target subscriber and the performed operation, or

some of them. The authorisation rules of the requested data shall be defined at least in the GUP Component level in GUP Server. (Note that the authorisation may be based on also on finer granularity of the data content.)

4.2.1.5 Synchronisation of Profile Components

In proxy mode, the GUP Server shall convey the data synchronisation requests from the applications to the RAFs in the same way as the other profile requests. Also the related change notifications from the RAFs are passed on to the requesting application. This requires that some kind of book keeping about the synchronisation requests implemented. In redirect mode the GUP server shall redirect the Application to the RAFs in the same way as the other profile requests.

The GUP Server may store a copy of the actual data from the GUP Data Repository, but it is up to the local policy of the GUP Server.

4.2.1.6 Additional Functionality

The GUP Server may take part in the charging of the data management operations concerning the profile.

The GUP Server may take part in the rate and/or size limiting of the data operations towards the profile.

4.2.2 Repository Access Function (RAF)

The Repository Access Function (RAF) realizes the Harmonised Access interface. It hides the implementation details of the data repositories from the GUP infrastructure. The RAF performs protocol and data transformation where needed.

The protocol between the RAF and the GUP data repository is out of the standardisation scope. It is recommended that the protocol used should support GUP requirements.

4.2.3 GUP Data Repository

Each GUP Data Repository stores the primary master copy of one or several profile components. The RAF provides for the standardised access to the GUP Data Repository. The storage formats or the interface between the RAF and GUP Data Repository are not specified by GUP. It is presumed that the RAF and the GUP Data Repository are usually co-located in the same network element.

4.2.4 Reference Points

Reference Points in the GUP Reference Architecture:

1. Reference Point Rg

This reference point shall allow applications to create, read, modify and delete any user profile data using the harmonized access interface. The GUP Server locates the data repositories responsible of the storage of the requested profile component(s) and in case of proxy mode carries out the requested operation on the data.

In the redirect mode, the GUP Server returns the locations of the GUP Data Repositories and the application can then send the requested operations via reference point Rp directly to the corresponding GUP Data Repositories.

The reference point Rg carries user related data, and therefore shall be protected by security mechanisms.

2. Reference Point Rp

This reference point shall allow the GUP Server or applications, excluding third party applications, to create, read, modify and delete user profile data using the harmonized access interface. Third party applications and third party GUP data repositories shall be connected to the GUP Server only using the Rg reference point.

The reference point Rp carries user related data, and therefore shall be protected by security mechanisms.

4.2.5 Applications

The applications that may apply GUP reference points Rg and Rp may be targeted for different purposes e.g. for value added services or subscription management. Both operator's own applications and third party applications are covered.

The latter ones shall apply Rg reference point. Applications have different authorisation rights to the GUP data of different subscribers as agreed between the parties.

4.2.6 Message Flow of using GUP

For an application requesting GUP data component(s) a message flow is described in the following:

- The application requests a GUP component(s) via Single Point of Access (Rg) from the GUP server. The application will indicate if it can support the Redirect mode.
- The GUP server authenticates the application. Note that also separate authentication services may be applied.
- The GUP Server identifies the level of authorization the Application is allowed to access the GUP data.
- The GUP Server identifies the location of the GUP component(s).

At this point the GUP Server may (see figure 4.5 below)

- Access the GUP component(s) by means of the Harmonised Access Interface (Rp) or by other means outside the scope of GUP.
- Respond to the application with the result of the request, optionally combining results from different GUP data repositories.

Or, depending on GUP data repositories choice and if the application has indicated that it can support the Redirect mode (see figure 4.6 below)

- Respond to the application with reference(s) to the component(s) and additionally authorisation credentials with limited lifetime. Note that authorisation credentials from other sources are not excluded.
- The application uses the reference(s) and the authorisation credentials to access GUP data repositories by means of the Rp reference point.

Privacy rules may stay together with the data it applies to at the data repository where the data is stored. In this case this privacy rules shall apply. Optionally, the GUP Server may apply additional privacy rules. However the GUP Server must never “bypass” existing privacy rules.

The following figures show the message flows for both cases as described.

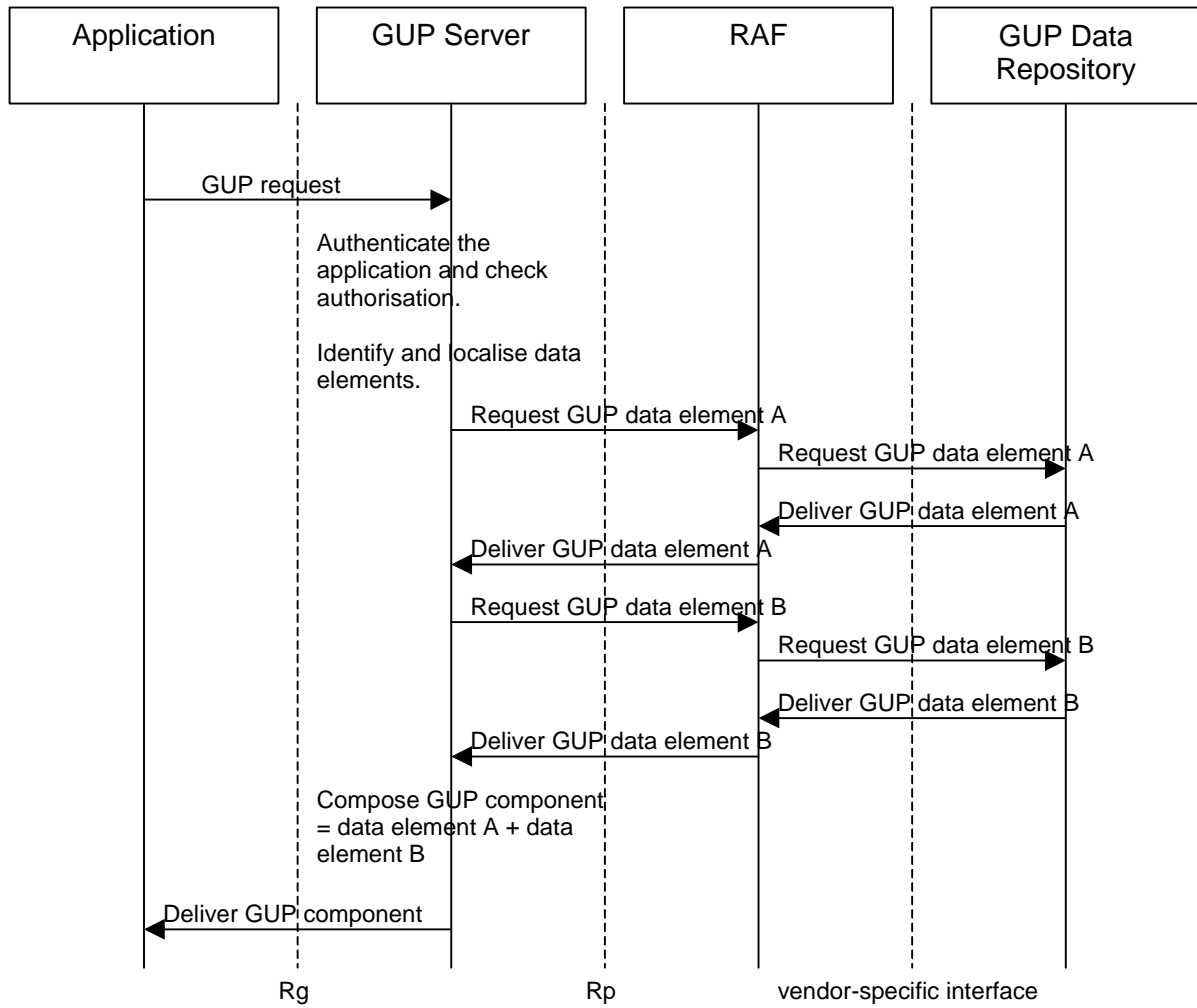


Figure 4.5: An Example of Application Requesting GUP Data Component(s) Message Flow (Proxy Mode)

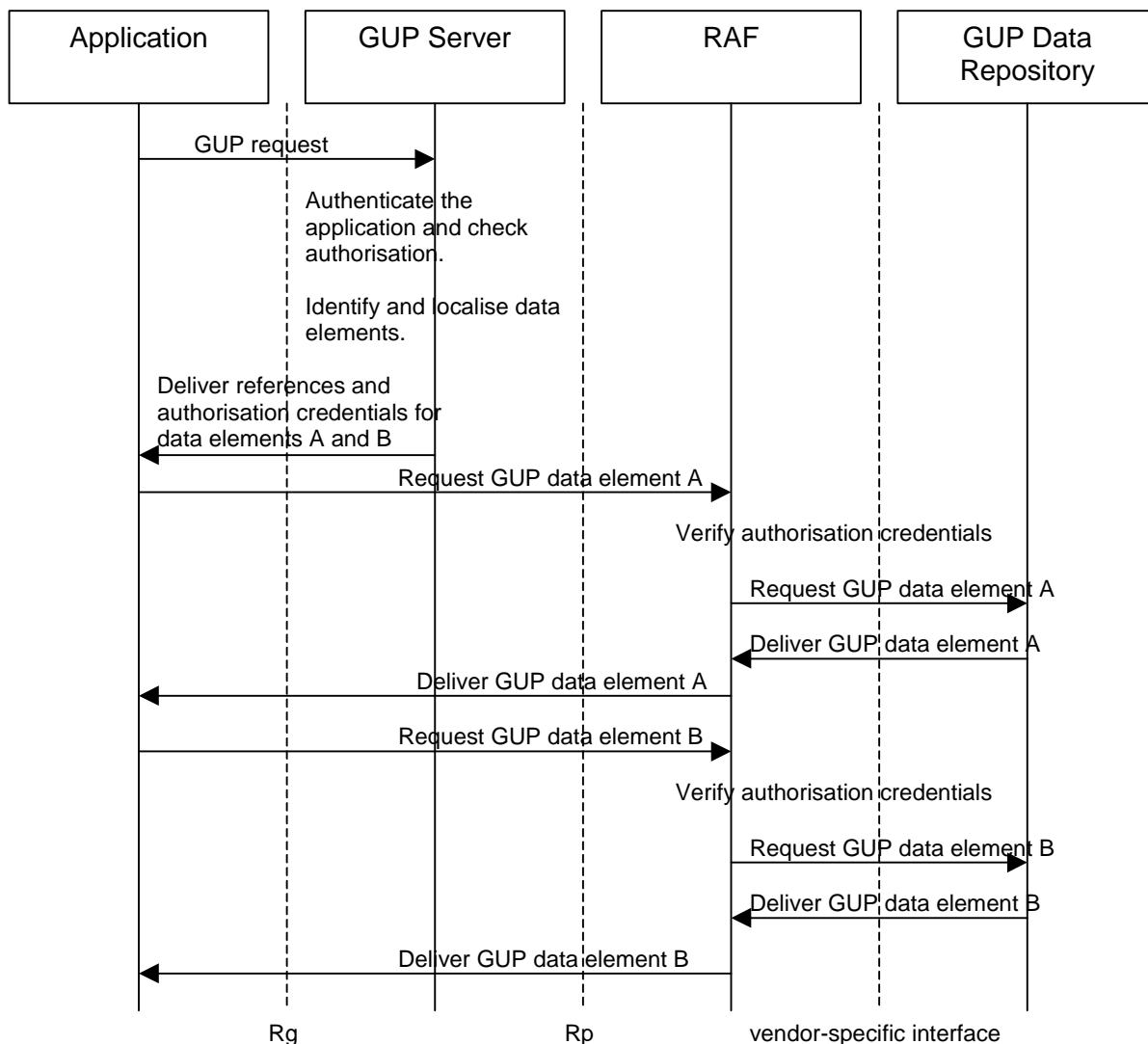


Figure 4.6: An Application Requesting GUP Data Component(s) Message Flow (Redirect Mode)

4.3 Rg reference point procedures

This subclause defines the procedures applied in the Rg reference point between the applications and the GUP Server. This reference point supports also third party profile access. Rg can be used e.g. to create the whole user profile or some components in it, to read any piece of data in the profile or to modify those. There are means to authorise all requests and protect the user’s privacy in all operations. Rg is applied to control the data stored in the different GUP components as per users.

There are the following procedures:

- Create
- Delete
- Modify
- Query
- Subscribe
- Unsubscribe

- Notify

4.3.1 Create procedure

Create procedure is used by the application to create a new user profile or new components to an existing profile. The procedure is always related to a single subscriber identity which is given in the request. Additionally the Create procedure shall carry the component types and the data to be created to each component. At least one component shall be provided. Creation of the first component implies profile creation. The component type identifies what data are concerned i.e. not just the data typing. It is presumed that the profile data structure is already known by the both parties. No new type of data can be defined by this procedure, only the data contents are provided. Furthermore the application shall provide the necessary data for authentication and authorisation of this create function (e.g. credentials, assertions and identifications).

The outcome of the procedure shall be provided in a separate response message.

Table 4.1: Request data of Create procedure

Parameter	Description	Use
Subscriber Identity	Specifies the user identity with its type (e.g. SIP URI public ID).	Mandatory
Component data	Specifies which components are addressed and provides the data for those. There may be several Component data elements corresponding to several created components. At least one element must be present. See the table below for the more detailed contents.	Mandatory
Requestor data	Specifies the data related to the requestor. These data may be used as input in the authentication and authorisation process. E.g. end user and application identification, credentials or privacy policy information.	Optional

Table 4.2: Contents of Component data parameter

Parameter	Description	Use
Component type	Specifies the type of the created component. The Component type identifies the applied component data definitions.	Mandatory
Data	Specifies the GUP component data according to the specified Component type.	Mandatory

Table 4.3: Response data of Create procedure

Parameter	Description	Use
Status	Indicates whether the procedure was carried out successfully or whether some failure was detected. The possible errors are described in sufficient detail.	Mandatory (like the response itself)

4.3.2 Delete procedure

Delete procedure is used by the application to remove a profile or selected GUP components from the repository. The attached subscriber identity and the component type are specified. If no component type is provided, the whole user profile identified by the Subscriber identity will be deleted. The application shall provide the necessary data for authentication and authorisation purposes (e.g. credentials, assertions and identifications).

The outcome of the procedure shall be provided in a separate response message.

Table 4.4: Request data of Delete procedure

Parameter	Description	Use
Subscriber identity	Specifies the user identity with its type (e.g. SIP URI public ID).	Mandatory
Component types	Specifies the types of the components.	Optional
Requestor data	Specifies the data related to the requestor. These data may be used as input in the authentication and authorisation process. E.g. end user and application identification, credentials or privacy policy information.	Optional

Table 4.5: Response data of Delete procedure

Parameter	Description	Use
Status	Indicates whether the procedure was carried out successfully or whether some failure was detected. The possible errors are described in sufficient detail.	Mandatory (like the response itself)

4.3.3 Modify procedure

Modify procedure is used by the application to change the data in the GUP components. Also adding and deleting data is possible by Modify procedure, but it cannot create a new component. The modified data are identified by the user identity and the data reference. The modification may concern the whole component or any lower level piece of data referenced in the procedure invocation. The contents for the entire referenced data shall be provided. Several individual changes to different components can be made with one procedure invocation. It must be noted that if modification of one component fails, the other changes cannot always be rolled back (implementation specific feature). However the response data shall specify which modifications were not accomplished. It is also possible to add more similar type of data elements to an existing array type of element. The requestor shall provide the necessary data for authentication and authorisation purposes (e.g. credentials, assertions and identifications).

The outcome of the procedure shall be provided in a separate response message.

Table 4.6: Request data of Modify procedure

Parameter	Description	Use
Subscriber identity	Specifies the user identity with its type (e.g. SIP URI public ID).	Mandatory
Modification data	Specifies which data are addressed and how those are changed. There may be several Modification data items corresponding to several individual modifications. These modifications may concern the same or different components. See the table below for the contents of one modification.	Mandatory
Requestor data	Specifies the data related to the requestor. These data may be used as input in the authentication and authorisation process. E.g. end user and application identification, credentials or privacy policy information.	Optional

Table 4.7: Contents of Modification data parameter

Parameter	Description	Use
Data reference	Specifies which data are modified or expanded. The reference identifies both the component type and the possible deeper level data reference. The reference must be unique in a way that it refers only to one data item.	Mandatory
New data	Specifies the data to be stored in the GUP component. It is expected that all the data elements in the referenced data structure are given.	Mandatory
Overwrite indication	Specifies if the data are added to the existing data or replaces those. Default action is "insert".	Optional

Table 4.8: Response data of Modify procedure

Parameter	Description	Use
Status	Indicates whether the procedure was carried out successfully or whether some failure was detected. The possible errors are described in sufficient detail.	Mandatory (like the response itself)

4.3.4 Query procedure

Query procedure is used by the application to retrieve the data in the user profile or its specific components. The queried data are identified by the user identity and the data reference. The data retrieval may concern the whole profile, component or any parts of a component as referenced in the invocation. The requestor shall provide the necessary data for authentication and authorisation purposes (e.g. credentials, assertions and identifications).

The retrieved data shall be provided in a separate response message.

Table 4.9: Request data of Query procedure

Parameter	Description	Use
Subscriber identity	Specifies the user identity with its type (e.g. SIP URI public ID).	Mandatory
Data references	Specifies which data are read. The data reference identifies the component type and the deeper level reference (if the whole component is not meant to be read). Multiple references may be given. It is also possible to refer to the profile root which implies that the whole profile data are queried.	Mandatory
Requestor data	Specifies the data related to the requestor. These data may be used as input in the authentication and authorisation process. E.g. end user and application identification, credentials or privacy policy information.	Optional

Table 4.10: Response data of Query procedure

Parameter	Description	Use
Data	Contains the retrieved data as indicated by the Data references.	Mandatory
Status	Indicates whether the procedure was carried out successfully or whether some failure was detected. The possible errors are described in sufficient detail.	Mandatory

4.3.5 Subscribe procedure

Subscribe procedure is used by the application to request notifications about changes in the GUP component data. The subscribed data are identified by the user identity and the data reference. Furthermore the application can identify which elements are to be monitored for changes if it is not interested in all changes. Data synchronisation can be performed by Subscribe and Notify procedures. The GUP Server returns the identification of the subscription request to provide means for the application to link the notifications of Notify procedure to the related subscribe requests.

A filtering data parameter is defined to facilitate performance optimisation. This may be left partly vendor/operator specific. The requestor shall provide the necessary data for authentication and authorisation purposes (e.g. credentials, assertions and identifications).

The outcome of the procedure shall be provided in a separate response message.

Table 4.11: Request data of Subscribe procedure

Parameter	Description	Use
Subscriber identity	Specifies the user identity with its type (e.g. SIP URI public ID).	Mandatory
Data references	Specifies which data are monitored for changes. The reference identifies both the component type and the possible deeper level data reference. Multiple references may be given. Any change within the referenced data structure causes a notification to be sent. If the parameter is absent, all modifications are notified.	Optional
Requestor data	Specifies the data related to the requestor. These data may be used as input in the authentication and authorisation process. E.g. end user and application identification, credentials or privacy policy information.	Optional
Filter data	Specifies additional conditions for sending notifications to optimise the performance e.g. when immediate synchronisation is not required. The parameter specifies also whether the initial data values are requested to be reported.	Optional

Table 4.12: Response data of Subscribe procedure

Parameter	Description	Use
Invoke identification	Contains the invoke identification assigned by the GUP Server for this request.	Mandatory
Status	Indicates whether the procedure was carried out successfully or whether some failure was detected. The possible errors are described in sufficient detail.	Mandatory (like the response itself)

4.3.6 Unsubscribe procedure

Unsubscribe procedure is used by the application to cancel one or several existing subscriptions. The outcome of the procedure shall be provided in a separate response message.

Table 4.13: Request data of Unsubscribe procedure

Parameter	Description	Use
Invoke identifications	Specifies one or several invoke identifications assigned by the GUP Server for the subscriptions.	Mandatory

Table 4.14: Response data of Unsubscribe procedure

Parameter	Description	Use
Status	Indicates whether the procedure was carried out successfully or whether some failure was detected. The possible errors are described in sufficient detail.	Mandatory (like the response itself)

4.3.7 Notify procedure

Notify procedure is invoked by the GUP Server when the data which was identified in Subscribe procedure changes or when the invoked Subscribe procedure requested sending of all the initial values of the referenced data. The procedure identifies the changed data and provides the new values.

The outcome of the procedure shall be provided in a separate response message.

Table 4.15: Request data of Notify procedure

Parameter	Description	Use
Invoke identification	Specifies the invoke identification assigned by the GUP Server for this subscription.	Mandatory
Notified data	Specifies which data are reported together with the data itself. Multiple pieces of data may be provided.	Mandatory

Table 4.16: Response data of Notify procedure (optional)

Parameter	Description	Use
Status	Indicates whether the procedure was carried out successfully or whether some failure was detected. The possible errors are described in sufficient detail.	Mandatory (however the whole response is optional)

4.3.8 Common information definitions

The information elements that are applied in several procedures of Rg reference point are described in this subclause.

4.3.8.1 Requestor data

The Requestor data contain the information that the sender of the request provides in order to facilitate the authentication and authorisation functions. The access control and user privacy functions work based on these data. Also an unspecified Additional info parameter is defined to carry data e.g. for monitoring or accounting purposes. All the elements are optional. However at least one shall be present if the parameter is applied.

Table 4.17: Requestor data

Element	Description	Use
Subscriber identification	Specifies the end user being served.	Optional
Application identification	Specifies the application being served. The GUP Server has to link the Application identification to the actual sender of the request by the appropriate means taking into account the applied security measures and domains.	Optional
Credentials	Contains authentication information.	Optional
Authorisation assertion	Contains the assertion for authorisation. The nature of the assertion must be for one time use to prevent replay and cut-and-paste attacks. E.g. digest or signature mechanisms may be applied.	Optional
Privacy policy	Information about the applied privacy policy.	Optional
Additional info	Additional unspecified information related to the requestor or request.	Optional

4.3.9 Error handling and common error types

The basic principle in error handling is that all errors in carrying out the procedures lead to complete abortion of the requested operation. However if e.g. multiple modifications with separate data references are made with one procedure invocation, it is possible that part of these are completed even if some would fail. The procedure error responses identify the error type together with more detailed information about the cause of the error.

The common error types which can be applied to all procedures contain:

Table 4.18: Common error types

Error	Description
Invalid operation	The operation is invalid or unsupported.
Invalid parameter	The given parameter of the operation is invalid.
Unauthorised operation	There was no authority for the requested operation.
Data unavailable	The requested data were not available.
Unexpected error	An unexpected error condition was met.

4.4 Rp reference point procedures

This subclause defines the procedures applied in the Rp reference point. The application or GUP server acts as the active requestor towards the Repository Access Function (RAF) entities e.g. to read or modify the data. It is assumed that the both ends share initially the same data structure definitions. Rp is applied to control the data stored in the different user profile components as per users. To address the data the user identity or the component identification is given accompanied with the lower level data reference when required.

There are the following procedures:

- Create Component
- Delete Component
- Modify Data
- Read Data
- Subscribe To Data
- Unsubscribe To Data
- Notify Data
- Define Data

Editor's note: How the existing profile components are included in the Generic User Profile is FFS.

4.4.1 Create Component procedure

Create Component procedure is used by the application to add a new profile component in the contacted repository. The attached user identity and the created component type are specified along with the created data. The component type identifies what data are concerned i.e. not just the data typing. It is presumed that the profile data structure is already known by the both parties. No new type of data can be defined by this procedure, only the data contents are provided. The requestor shall provide the necessary data for authorisation purposes (e.g. assertions and identifications).

This procedure is synchronous in nature but it is also possible to define a separate response message.

Table 4.19: Request data of Create Component procedure

Parameter	Description	Use
Subscriber Identity	Specifies the user identity with its type (e.g. SIP URI public ID).	Mandatory
Component type	Specifies the type of the created component. This is needed because several types may be supported by one RAF. The Component type identifies the applied component data definitions.	Mandatory
Requestor data	Specifies the data related to the requestor. These data may be used as input in the authorisation process. E.g. end user and application identification. See subclause 4.4.9.	Optional
Component data	Specifies the profile component data according to the specified Component type.	Mandatory

Table 4.20: Response data of Create Component procedure

Parameter	Description	Use
Status	Indicates whether the procedure was carried out successfully or whether some failure was detected. The possible errors are described in sufficient detail.	Mandatory (like the response itself)

4.4.2 Delete Component procedure

Delete Component procedure is used by the application to remove a profile component from the contacted repository. The attached user identity and the component type is specified. The requestor shall provide the necessary data for authorisation purposes (e.g. assertions and identifications).

This procedure is synchronous in nature but it is also possible to define a separate response message.

Table 4.21: Request data of Delete Component procedure

Parameter	Description	Use
Subscriber identity	Specifies the user identity with its type (e.g. SIP URI public ID).	Mandatory
Component type	Specifies the type of the component.	Mandatory
Requestor data	Specifies the data related to the requestor. These data may be used as input in the authorisation process. E.g. end user and application identification. See subclause 4.4.9.	Optional

Table 4.22: Response data of Delete Component procedure

Parameter	Description	Use
Status	Indicates whether the procedure was carried out successfully or whether some failure was detected. The possible errors are described in sufficient detail.	Mandatory (like the response itself)

4.4.3 Modify Data procedure

Modify Data procedure is used by the application to change the data in a profile component. The component is identified by the user identity and the component type. The modification may concern the whole component or any lower level piece of data referenced in the procedure invocation. The contents for the entire referenced data shall be provided. Several individual changes to the component can be made with one procedure invocation. It is also possible to add more similar type of data elements to an existing array type of element. The requestor shall provide the necessary data for authorisation purposes (e.g. assertions and identifications).

This procedure is synchronous in nature but it is also possible to define a separate response message.

Table 4.23: Request data of Modify Data procedure

Parameter	Description	Use
Subscriber identity	Specifies the user identity with its type (e.g. SIP URI public ID).	Mandatory
Component type	Specifies the type of the component.	Mandatory
Modified data	Specifies which data are addressed and how those are changed. There may be several modified data items corresponding to several individual modifications. See the table below for the contents of one modification.	Mandatory
Requestor data	Specifies the data related to the requestor. These data may be used as input in the authorisation process. E.g. end user and application identification. See subclause 4.4.9.	Optional

Table 4.24: Contents of Modified data parameter

Parameter	Description	Use
Data reference	Specifies which data are modified or expanded. The reference may indicate the whole component or any deeper level piece of data. The reference must be unique in a way that it refers only to one data item.	Mandatory
New data	Specifies the data to be stored in the profile component. It is expected that all the data elements in the referenced data structure are given.	Mandatory
Overwrite indication	Specifies if the data are added to the existing data or replaces those. Default action is "insert".	Optional

Table 4.25: Response data of Modify Data procedure

Parameter	Description	Use
Status	Indicates whether the procedure was carried out successfully or whether some failure was detected. The possible errors are described in sufficient detail.	Mandatory (like the response itself)

4.4.4 Read Data procedure

Read Data procedure is used by the application to retrieve the data in a profile component. The component is identified by the user identity and the component type. The data retrieval may concern the whole component or any parts of it as referenced in the invocation. The requestor shall provide the necessary data for authorisation purposes (e.g. assertions and identifications).

Table 4.26: Request data of Read Data procedure

Parameter	Description	Use
Subscriber identity	Specifies the user identity with its type (e.g. SIP URI public ID).	Mandatory
Component type	Specifies the type of the component.	Mandatory
Data references	Specifies which data are read. The data reference may point to a piece of data on any level in the data structure (also to the whole component). Multiple references may be given.	Mandatory
Requestor data	Specifies the data related to the requestor. These data may be used as input in the authorisation process. E.g. end user and application identification. See subclause 4.4.9.	Optional

Table 4.27: Response data of Read Data procedure

Parameter	Description	Use
Data	Contains the retrieved data as indicated by the Data references. All the data under the referenced one are returned. Multiple packets of data are given if so requested.	Mandatory
Status	Indicates whether the procedure was carried out successfully or whether some failure was detected. The possible errors are described in sufficient detail.	Mandatory (like the response itself)

This procedure is synchronous in nature but it is also possible to define a separate response message.

4.4.5 Subscribe To Data procedure

Subscribe To Data procedure is used by the application to request notifications about changes in the profile component data. The component is identified by the user identity and the component type. Furthermore the application can identify which elements are to be monitored for changes if it is not interested in all changes. Data synchronisation can be

performed by Subscribe To Data and Notify Data procedures. The RAF returns the identification of the subscription request to provide means for the application to link the notifications of Notify Data procedure to the related subscribe requests.

A filtering data parameter is defined to facilitate performance optimisation. This may be left partly vendor/operator specific. The requestor shall provide the necessary data for authorisation purposes (e.g. assertions and identifications).

Table 4.28: Request data of Subscribe To Data procedure

Parameter	Description	Use
Subscriber identity	Specifies the user identity with its type (e.g. SIP URI public ID).	Mandatory
Component type	Specifies the type of the component.	Mandatory
Data references	Specifies which data are monitored for changes. Multiple references may be given. Any change within the referenced data structure causes a notification to be sent. If the parameter is absent, all modifications are notified.	Optional
Requestor data	Specifies the data related to the requestor. These data may be used as input in the authorisation process. E.g. end user and application identification. See subclause 4.4.9.	Optional
Filter data	Specifies additional conditions for sending notifications to optimise the performance e.g. when immediate synchronisation is not required. The parameter specifies also whether the initial data values are requested to be reported.	Optional

Table 4.29: Response data of Subscribe To Data procedure

Parameter	Description	Use
Invoke identification	Contains the invoke identification assigned by the RAF for this request.	Mandatory
Status	Indicates whether the procedure was carried out successfully or whether some failure was detected. The possible errors are described in sufficient detail.	Mandatory (like the response itself)

4.4.6 Unsubscribe To Data procedure

Unsubscribe To Data procedure is used by the application to cancel one or several existing subscriptions.

Table 4.30: Request data of Unsubscribe To Data procedure

Parameter	Description	Use
Invoke identifications	Specifies one or several invoke identifications assigned by the RAF for the subscriptions.	Mandatory

Table 4.31: Response data of Unsubscribe To Data procedure

Parameter	Description	Use
Status	Indicates whether the procedure was carried out successfully or whether some failure was detected. The possible errors are described in sufficient detail.	Mandatory (like the response itself)

4.4.7 Notify Data procedure

Notify Data procedure is invoked by the RAF when the data which was identified in Subscribe To Data procedure changes or when the invoked Subscribe To Data procedure requested sending of all the initial values of the referenced data. The procedure identifies the changed data and provides the new values.

Table 4.32: Request data of Notify Data procedure

Parameter	Description	Use
Invoke identification	Specifies the invoke identification assigned by the RAF for this subscription.	Mandatory
Notified data	Specifies which data are reported together with the data itself. Multiple pieces of data may be provided.	Mandatory

Table 4.33: Response data of Notify Data procedure (optional)

Parameter	Description	Use
Status	Indicates whether the procedure was carried out successfully or whether some failure was detected. The possible errors are described in sufficient detail.	Mandatory (however the whole response is optional)

4.4.8 Define Data procedure

Define Data procedure is used by the application to define new data elements to the profile component data structure. The names and types for the new data are specified. This procedure facilitates extension of the profile data with new, proprietary data. Subsequently these data can be handled by the above described procedures e.g. modified by the Modify Data procedure.

4.4.9 Common information definitions

The information elements that are applied in several procedures are described in this subclause.

4.4.9.1 Requestor data

The Requestor data contain the information that the sender of the request provides in order to facilitate the authorisation functions. The access control and user privacy functions work based on these data. Also an unspecified Additional info parameter is defined to carry data e.g. for monitoring or accounting purposes. All the elements are optional. However at least one shall be present if the parameter is applied.

Table 4.34: Requestor data

Element	Description	Use
Subscriber identification	Specifies the end user being served.	Optional
Application identification	Specifies the application being served. The RAF has to link the Application identification to the actual sender of the request by the appropriate means taking into account the applied security measures and domains.	Optional
Authorisation assertion	Contains the assertion for authorisation. The nature of the assertion must be for one time use to prevent replay and cut-and-paste attacks. E.g. digest or signature mechanisms may be applied. The provisioning of the assertions or any related shared secrets is beyond Rp reference point specifications.	Optional
Additional info	Additional unspecified information related to the requestor or request.	Optional

4.4.10 Error handling and common error types

The basic principle in error handling is that all errors in carrying out the procedures lead to complete abortion of the requested operation. The procedure error responses identify the error type together with more detailed information about the cause of the error.

The common error types which can be applied to all procedures contain:

Table 4.35: Common error types

Error	Description
Invalid operation	The operation is invalid or unsupported.
Invalid parameter	The given parameter of the operation is invalid.
Unauthorised operation	There was no authority for the requested operation.
Data unavailable	The requested data were not available.
Unexpected error	An unexpected error condition was met.

5 GUP Information Model

A Generic User Profile consists of a number of independent GUP Components.

The GUP Component has a unique identity within the Generic User Profile, and it can be retrieved through one RAF.

A GUP Component contains zero or more Data Element Groups. The Data Element Group contains indivisible Data Elements and/or Data Element Groups. The nested Data Elements Groups allow deeper hierarchial structures. The Data Element Group in the lowest hierarchical level contains one or more Data Elements. The Data Element Groups inside a GUP Component may be of the same or different types.

Alternatively the GUP Component may contain zero or more Data Elements without the Data Element Groups. A GUP component shall have at least one Data Element Group or Data Element.

A Composite Datatype is used to define the structure of the whole GUP Component. The structure includes definition about what kind of Data Element Groups and/or which Data Elements belong to the defined GUP Component as well as the data types and valid values of the data.

The UML Class Diagram below illustrates the basic concepts of the GUP Information Model.

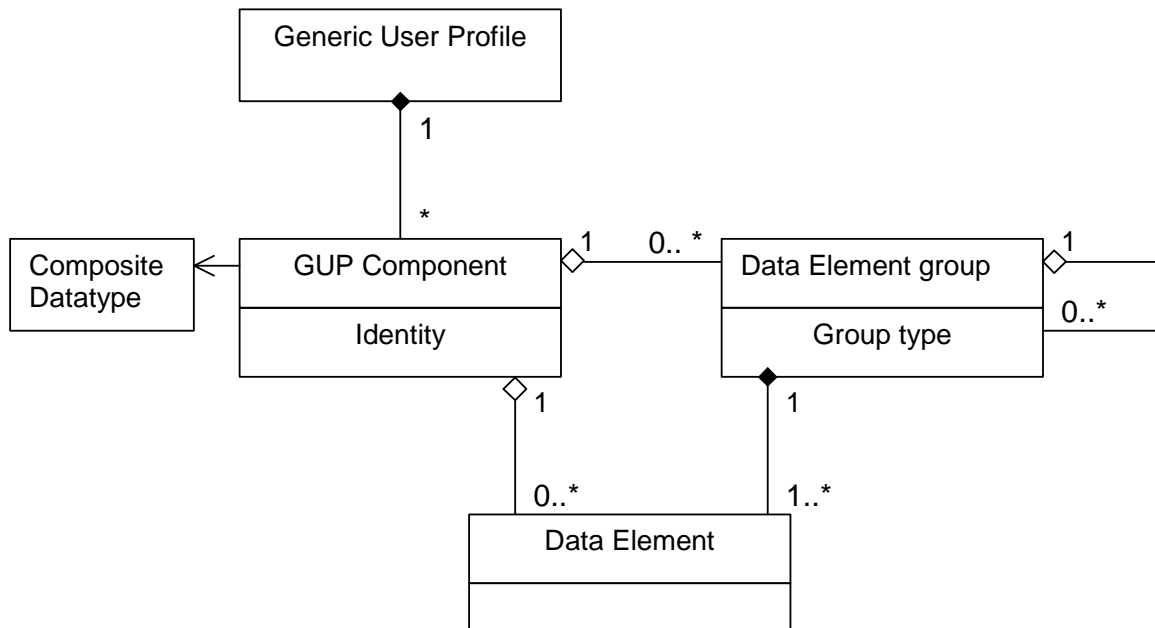


Figure 5.1: The basic concepts of GUP

Editor’s note: Whether the authorisation and privacy related enhancements have effect on the information model is FFS.

Figure 5.2 presents an example structure of Generic User Profile with the terms used in the UML Class Diagram. Note that the data structure may be also deeper than shown in the example figure, e.g., the Data Element Groups might consist of nested Data Element Groups.

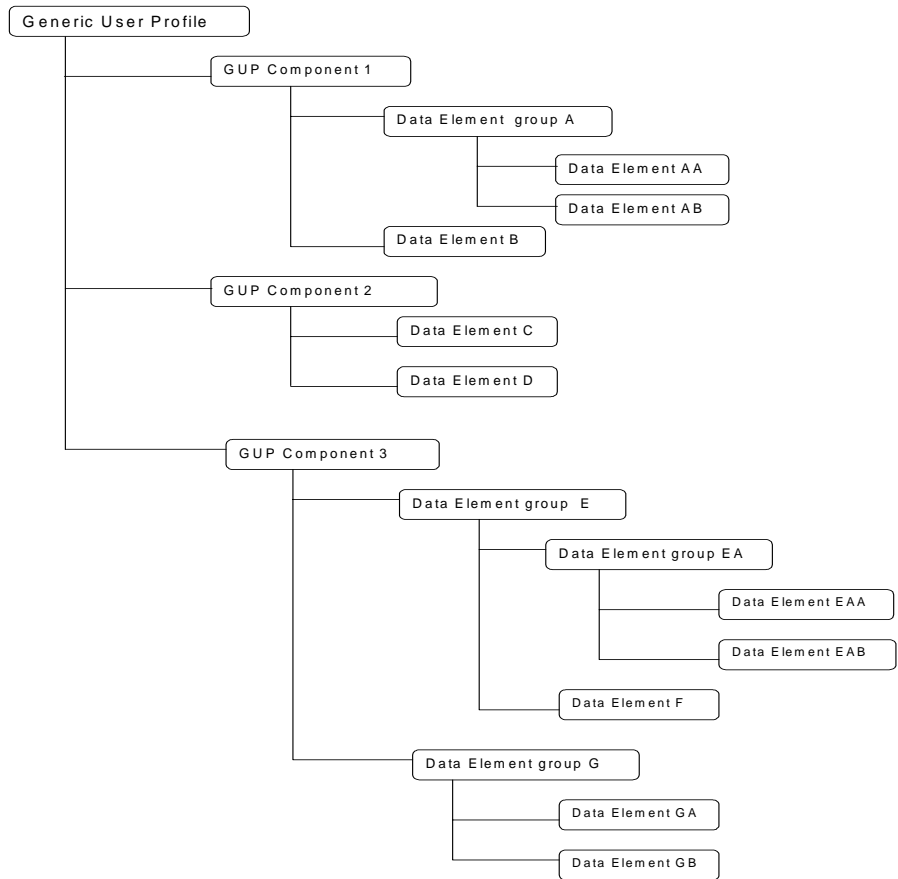


Figure 5.2: Example structure of GUP information

One purpose of the example structure is to clarify the intended relation between the UML Class Diagram and the hierarchical structure of GUP in terms of XML.

Each Generic User Profile consists of one or several GUP Components depending on the nature of the user related data. GUP Components are independent XML documents. The Generic User Profile is thus formed of a number of XML documents.

Each GUP Component consists of Data Elements and/or Data Element Groups as defined in the component specific definitions. In XML terms the Data Elements are XML elements. The Data Element Group is a structured XML element with an arbitrarily deep data structure.

Annex A (informative): Examples of 3GPP Generic User Profile Usage

Example 1: GUP Interworking with Device Management

As the device management specification 32.802 requests, the UEM Gateway controls the access available to the UE managers. The GUP server will perform gateway functionality for device management. The example of the interworking interface diagram is shown in Figure A.1.

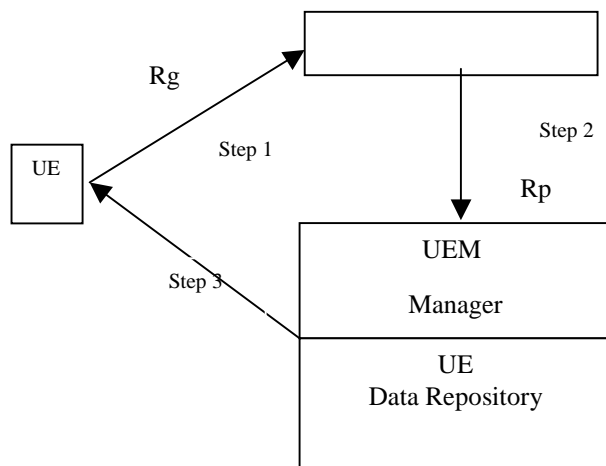


Figure A.1: An Example of the Interworking Diagram between GUP and Device Management

The interworking steps between GUP and Device management are summarised below:

Step 1: GUP Server allows any requests from UE to be accessed in a secured manner.

Step 2: GUP Server routes the request from UE to the appropriate UE management within the data repository.

Step 3: Data transactions take place.

NOTE: In this example the GUP server is working in proxy mode, this does not preclude the possibility for the GUP server to work in redirect mode when interworking with Device Management.

Annex B (informative): 3GPP Generic User Profile candidates

This table lists the Generic User Profile candidates grouped per GUP access. It gives for each data access, the supplier, the consumer and the data repository. The applied categorisation of the data in the table does not imply similar GUP component structure.

GUP access	Supplier	Data repository	Description of the data	Consumer
Terminal related data for CS, PS, IMS	UE manager	UE-USIM/ISIM	Terminal capabilities of the terminal in use: - MS classmark 1, 2, 3 - User interface capability - Communication capabilities Data for initial configuration and/or reset of the ME Backup data for recovery of the ME Configuration including service specific data	MSC/VLR SGSN GGSN S-CSCF
General user data for CS & PS	UE manager	UE-USIM	USIM user data for CS&PS: - Language indicator - IMSI - Phone books - available services - service capabilities	MSC/VLR SGSN GGSN
General user data for IMS	UE manager AS manager	UE-USIM/ISIM AS	ISIM subscriber data for IMS: - Private & Public SIP URI of the user - Settings back up/restore - Preferences (e.g. languages) - Phone books - Buddy list - Available services - Service capabilities - Active service profile	UE-USIM/ISIM S-CSCF AS
MMS terminal capability negotiation Ref 31.102, 23.140	UE manager	MMS-UA	MMS terminal capability information: - maximum supported size of an MM - maximum supported resolution of an image - list of supported media types and media formats (e.g. MIME types) - list of supported character sets - list of preferred languages - maximum supported colour depth - indication whether or not the recipient MMS User Agent supports streaming for the retrieval of MM contents	MMS server
MMS VASP applications Ref 23.141	AS manager	AS	MMS application specific data: - Authorization - Confidentiality - Charging information - Message distribution	MMS server
Privacy control settings of the user	AS manager	AS	Privacy control data of the user: - Privacy settings for standardised service like Presence - Privacy setting of non standardised services	UE-ISIM
PLMN specific user information	O&M	HSS	PLMN specific user information: - User addresses (e.g. MSISDNs, URLs) - WAP parameters (e.g. standard WAP gateway) - GPRS parameters - Preferred access technologies (e.g. UTRAN, GERAN, WLAN etc...)	S-CSCF AS
Authorised and subscribed service information for CS & PS	O&M HSS-HLR	HSS-HLR	Authorised and subscribed service information: - Subscriber ID (IMSI, MSISDNs) - General subscription information - Subscription restrictions - Basic & Supplementary services - Charging plans - Operator determined barring data is FFS - SMS subscription - MMS subscription	MSC/VLR GMSC SGSN GGSN MMS server
CSE handling of user subscriptions for CS & PS	CSE	HSS-HLR	- Forwarding & barring information - CAMEL subscription information	CSE

Authorised and subscribed service information for IMS	O&M	HSS	Authorised and subscribed service information: <ul style="list-style-type: none">- IM Subscriber ID (Private User ID, Public ID)- Subscribed media- Billing policy- Initial filter criteria- Service keys & triggering aspects- Authorised services that the subscriber may subscribe to- Services the subscriber actually has subscribed to	S-CSCF AS
CAMEL services for IMS	O&M	HSS-HLR	CAMEL subscription information for IMS	IM-SSF

Annex C (informative): Change history

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
01-11-13		UP-010103			First version of the draft specification from UP-010065		
01-11-14		UP-010109			After UP#6 V0.2.0		
01-12-05		UP-010136			After UP#7 V0.3.0 Added changes from UP-010116 , UP-010134 and UP-010135 Reference added to GUP stage 1 TS 22.240 Chapter 8 moved under chapter 4 Chapter 10 moved to Annex A Editorial changes		
02-02-19		S2-020705			Outcome of SA2#23, version 0.4.0 with revision marks		
02-02-19		S2-020706			Outcome of SA2#23, version 0.4.1 clean copy		
02-06-25		S2-021881			Updates from SA2 drafting session		
02-06-25		S2-021882			Outcome of SA2#25, version 0.5.1 clean copy		
02-08-22		S2-022487			Outcome of SA2#26, version 0.6.0 with revision marks		
02-08-22		S2-022487			Outcome of SA2#26, version 0.6.1 clean copy		
02-10-15		S2-023067			Outcome of SA2#27, version 0.7.0 with revision marks		
02-10-15		S2-023067			Outcome of SA2#27, version 0.7.1 clean copy		
02-11-15		S2-023499			Outcome of SA2#28, version 0.8.0		
02-11-20		S2-023499r1			SA2#28 e-mail approval, version 0.9.0		
03-01-24		S2-030439			Outcome of SA2#29, version 0.10.0		
03-02-05		S2-030439r2			SA2#29 e-mail approval, version 0.11.0		
03-03-07		S2-030944			Produced for TSG-SA#19. Outcome of SA2#30 version 0.12.0.		
03-04-11		S2-031551			Outcome of SA2#31, version 1.1.0		
03-05-26		S2-032170			Outcome of SA2#32, version 1.2.0		
03-05-26		S2-032171			Version 2.0.0, clean copy of version 1.2.0		